Reclamation Manual

Directives and Standards

Examples of Reclamation FOUO Information

- Documents that describe the ways of entering or accessing critical areas at a specific facility or methods of operating that facility. The term "critical" is generally intended to refer to any location at a facility where an unauthorized intruder could disrupt the operation, function, or mission of the facility. This includes:

  - Standing Operating Procedures and Designers' Operating Criteria.
  - Operating procedures related to equipment at a dam, powerplant, or other facility including equipment operating procedures, locations, and drawings.
  - Information related to the supervised remote control of a specific facility. This includes SCADA documentation, operational drawings, designs, computer source code, communication/control procedures, and protocols for key structures such as dams, powerplants, pumping plants, and waterway systems.

- Sensitive communications, organizational, and operational information, such as:

  - Personal or restricted-use telephone numbers.
  - Privacy Act information.
  - Staffing levels related to specific facilities or resources.
  - Specific information about staff in sensitive, law enforcement, or management positions.
  - Continuity of Operations (COO) Plans, Emergency Action Plans (EAP), and related information such as inundation maps.

- Tables and general descriptions of Reclamation's threat condition protective measures.

- Portions of facility review reports (periodic facility reviews/comprehensive facility reviews) for specific dams, powerplants, etc., that describe failure modes or specific structural vulnerabilities of the facilities that could be used by an unauthorized intruder to cause damage or harm to the facility.

- Dam safety information such as:

  - Risk analyses, including failure probabilities, failure consequences and damage estimates, risk calculations, and related estimates from normal loading conditions, seismic events, and floods.
  - Improvement or vulnerability mitigation recommendations (related to facilities, features, or other resources).
  - Agency decisions regarding actions to address recommendations.
  - Documentation of activities to address recommendations (prior to completion of issue evaluation).

- Internal financial, budget, and draft policy information that would not be appropriate for public disclosure until deemed finalized and releasable by the agency. Budget information for security upgrades to specific features or resources.

The following types of FOUO information are considered higher sensitivity information requiring additional protective measures (see Paragraph 7.G.):

- Any information related to security risk management such as security risk analysis, security reviews, security assessments, security surveys, security evaluations, and security plans regarding specific facilities, such as:

  - Vulnerabilities of specific assets, including natural and man- made vulnerabilities, which are humanly exploitable and could result in significant or catastrophic consequences.
  - Documents that describe the potential consequences associated with the loss or failure of a specific dam or associated feature of the dam resulting from an attack by a human aggressor.
  - Recommendations/descriptions for security actions and/or countermeasures to mitigate vulnerabilities to a specific resource that describe how and why the action/measure is recommended or in place.

- SCADA security information.

- Security prioritization information and supporting data.

- Drawings, designs, specifications, and other engineering data related to specific security systems or measures.

- Site security plans.

- Specific responses to threat condition protective measures, such as number of guards, schedules, locations, etc.